CLAIMS

What is claimed is:

1. A method of protecting an electronic network, comprising:

installing one or more agents within components of the electronic network;

performing an initial assessment of the electronic network to determine normal activity;

monitoring the electronic network for abnormal activity using the agents; and

protecting the electronic network by blocking the abnormal activity using the agents.

2. The method of claim 1, wherein the step of installing comprises the step of installing a type 2 super peer agent for authorizing and reauthorizing the agents.

3. The method of claim 1, further comprising logically connecting at least one of the agents into one or more cooperative agent cells.

4. The method of claim 3, wherein the step of installing further comprises:

establishing bidirectional communication protocols for agent communication within the cooperative agent cells;

delegating one or more agents in the cooperative agent cells to have bidirectional communication with another delegated agent; and

establishing bidirectional communication protocols for each delegated agent to communicate with another delegated agent.

5. The method of claim 1, wherein the step of installing further comprises:

broadcasting a request for agents to submit to authentication; and

authenticating submitted agents.

6. The method of claim 3, wherein the step of logically connecting further comprises self-organizing at least one of the agents into each of the cooperative agent cells.

7. The method of claim 4, wherein the step of establishing further comprising communicating via at least one covert communication protocol.

8. The method of claim 1, wherein the step of performing an initial assessment comprises:

mapping systems, communication ports and attached devices of the electronic network; and

establishing normal activity of the systems, communication ports, and attached devices.

9. The method of claim 1, wherein the step of monitoring comprises:

non-destructively intercepting communications on the electronic network;

collecting events from the intercepted communications; and

determining if the events indicate abnormal activity.

10. The method of claim 1, wherein the step of protecting comprises one or more of:

luring a malicious agent that causes abnormal activity into a false appearance of success;

planting instructions on information retrieved by the malicious agent to assist in identifying the origins of the malicious agent;

isolating electronic network components which have been compromised by the malicious agent;

attacking the malicious agent;

formulating a strategy to eliminate recently discovered vulnerabilities in the electronic network;

installing patches to eliminate vulnerabilities in the electronic network;

reassessing the electronic network to detect abnormal operations; and

investigating abnormal operations of the electronic network.

11. The method of claim 3, further comprising promoting one of the agents in each of the cooperative agent cells to a cell delegate.

12. The method of claim 11, further comprising:

promoting a second agent in each of the cooperative agent cells to a type 1 super peer agent;

authenticating new agents with the type 1 super peer agent; and

communicating between the cooperative agent cells and a command and control console via the cell delegate to protect the network from malicious activity.

13. The method of claim 3, the agents and cooperative agent cells being configured for independent and collaborative investigation of the electronic network, isolation of compromised components of the electronic network, and defense of the electronic network.

14. A system for protecting an electronic network, comprising:

a plurality of agents with the electronic network, the agents being grouped into at least one cooperative agent cell having one cell delegate;

a communications protocol within each cooperative agent cell, for (a) communicating between agents of the cooperative agent cell, and (b) communicating with cell delegates external to the cooperative agent cell;

means for determining normal activity levels of the electronic network;

means for detecting malicious activity;

means for isolating compromised components of the electronic network;

means for counter-intelligence to reveal the origin of the malicious activity;

means for repairing damage caused by the malicious activity;

means for determining vulnerabilities in the current protection provided by the plurality of agents; and

means for improving protection to resist future attack on the electronic network.

15. A system for event monitoring, comprising:

an electronic network for collecting events;

one or more event correlation engines, each event correlation engine being connected to the electronic network and having a receive event handler for receiving events addressed to the event correlation engine; and

one or more event correlation modules, each of the event correlation modules having an event pattern that defines events of interest, each of the correlation modules receiving all events received by the event correlation engine, the event correlation module correlating the events of interest.

16. The system of claim 15, wherein the event correlation module is a simulated annealing correlator module.

17. The system of claim 16, the simulated annealing correlator further comprising:

recorded events;

a simulated annealing correlator engine;

heuristics; and

a correlation threshold;

wherein the simulated annealing correlator engine utilizes the heuristics and the correlation threshold to correlate the events received by the event correlation engine with the recorded events, the correlated events being added to the recorded events.

18. A method of pattern recognition, comprising:

collecting electronic network events;

sampling the electronic network events with one or more event correlation engines;

passing sampled electronic network events from each event correlation engine to one or more event correlator modules within each event correlation engine;

comparing events in each of the event correlator modules by sampling the events, determining if any of the events matches an event pattern, and, if there is a match, creating a new event announcing the match and passing the new event to the associated event correlation engine for electronic network distribution; and

determining patterns in events using a simulated annealing correlator, determining if the pattern is important, and, if so, creating a new event announcing the important pattern and passing the new event to the associated event correlation engine for network distribution.

19. The method of claim 18, wherein the step of sampling further comprises sampling all of, or less than all of, the electronic network events.